# Reforming the Mutual Legal Assistance Treaty Framework To Protect the Future of the Internet

JOE BARTON*

TABLE OF CONTENTS



* J.D. Candidate 2019, The Ohio State University Moritz College of Law. I would like to thank Professor Christopher J. Walker for the work he does teaching and connecting his students with federal agencies in Washington D.C. I also owe a huge debt of gratitude to Rachel Elwood, Maggie O'Shea, Hannah Barlow, Clair Bullock, Chance Johnson, and Scott Herkamp for all of the work that they put into helping ready this piece for publication.

## I. INTRODUCTION

The current system through which foreign law enforcement agencies request electronic data during the course of criminal investigations is broken. Foreign governments have grown frustrated as their efforts to investigate crimes and apprehend criminals have been thwarted by inefficiencies and delays in the data-request process. These inefficiencies have prompted foreign governments to engage in a number of behaviors that threaten human rights and disrupt the free flow of information across borders. Accordingly, the United States must assume a position of leadership by amending its privacy laws to fix the myriad problems which currently exist in the contemporary Internet privacy regime. This Essay examines the current reality of Internet usage worldwide, assesses the current international data-sharing regime, surveys potential avenues for the reform of that regime, and ultimately recommends that the United States take a measured and intentional approach towards reform.

More than three billion citizens of the world are connected to the Internet, via an estimated thirteen billion different devices.[1] The past decade has seen a marked shift towards utilizing cloud storage of Internet data,[2] which results in the remote storage of data on huge servers owned by Internet Service Providers (ISPs) and their affiliates.[3] The storage location that a particular piece of data is sent to depends on a number of factors, including proximity to the user, availability of server space, and cost.[4] Estimates suggest that within this decade, over half of the consumer Internet population will use cloud storage, and that nearly all data processing will happen in cloud data centers.[5] While the United States accounts for only about 9% of the world's Internet users, a substantial majority of the most popular websites and services are run by American firms, and thus governed by American communications laws.[6]

The Electronic Communications Privacy Act (Privacy Act), which was written in 1986, extends government restrictions on transmissions of electronic data and includes sections pertaining to wiretapping (the Wiretap Act), stored communications (the Stored Communications Act), and tracing telephone communications (the Pen/Trap Statute).[7] In short, the Privacy Act contains

---

[1] THE CHERTOFF GRP., LAW ENFORCEMENT ACCESS TO EVIDENCE IN THE CLOUD ERA 2, https://chertoffgroup.com/files/docs/LawEnforcement.pdf [https://perma.cc/UBN8-SJJ7].

[2] Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729, 740–41 (2016).

[3] *See id.* at 732, 744.

[4] THE CHERTOFF GRP., *supra* note 1, at 3.

[5] *See* Woods, *supra* note 2, at 741 (noting an estimate from the Cisco Global Cloud Index that "by 2019, 55% of the consumer Internet population will use personal cloud storage and 86% of data processing will happen remotely").

[6] *See id.* at 741, 743 n.71.

[7] *See* 18 U.S.C. §§ 2510–22 (2012); U.S. DEP'T OF JUSTICE, *Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510–22*, JUST. INFO. SHARING, https://www.it.ojp.gov/PrivacyLiberty/authorities/statutes/1285 [https://perma.cc/G6CJ-RHW5] (last updated July 30, 2013).

provisions which regulate the storage and transfer of data and prevent American data holders, via a blocking provision, from sharing information with foreign law enforcement agencies.[8] Therefore, when law enforcement agencies in foreign countries want access to stored communications from (mostly) American ISPs, they must seek that data through a decades-old request process, Mutual Legal Assistance Treaties (MLATs).[9] Upon being denied access to American-held data, a foreign law enforcement agency will file a formal Mutual Legal Assistance (MLA) request for the data through the U.S. Department of Justice's Office of International Affairs (OIA).[10] OIA prepares the request and forwards it along to the U.S. Attorney's Office (USAO).[11] The USAO then presents the MLAT request to a federal magistrate judge, who reviews the request under the Fourth Amendment probable cause standard required for a warrant.[12] If the warrant request is granted, the U.S. Federal Bureau of Investigation presents the warrant to the ISP who then passes the relevant data *back* to the Department of Justice for a final review before the Department of Justice turns it over to the requesting country.[13] This process takes about ten months on average.[14] Foreign law enforcement agency requests have skyrocketed since 2000, exacerbating the delay in MLAT request responses.[15] Indeed, the U.K. government alone made over 22,000 separate MLA requests to just six of the largest U.S. technology companies.[16] Foreign law enforcement agencies have repeatedly insisted that large numbers of investigations and cases are abandoned because there is no realistic possibility of obtaining the necessary data.[17] There are also claims that shortcomings in the MLA request process have created safe havens for cyber criminality in places like Eastern Europe, where cybercrime enforcement is not prioritized and Western countries lack jurisdiction to intervene.[18]

---

[8] Jennifer Daskal, *Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues*, 8 J. NAT'L SECURITY L. & POL'Y 473, 491 (2016).

[9] *See* Peter Swire & Justin D. Hemmings, *Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program*, 71 N.Y.U. ANN. SURV. AM. L. 687, 697–700 (2017) (explaining how MLATs work and the process of making an MLA request).

[10] *Id.* at 697–98.

[11] *Id.* at 698.

[12] *Id.* at 698–99.

[13] *Id.* at 699–700.

[14] *Id.* at 700.

[15] Woods, *supra* note 2, at 750.

[16] *Id.* at 743–44.

[17] AD-HOC SUBGROUP ON TRANSBORDER ACCESS & JURISDICTION, CYBERCRIME CONVENTION COMM. (T-CY), *Transborder Access to Data and Jurisdiction: Options for Further Action by the T-CY* 12 (Dec. 2014) [hereinafter CYBERCRIME CONVENTION COMM. (T-CY)], https://rm.coe.int/16802e726e [https://perma.cc/4C8Z-ADHU].

[18] THE CHERTOFF GRP., *supra* note 1, at 5.

## II. MLAT PROBLEMS

The cumbersome MLAT process has served as a catalyst, or at least as a justification, for a number of troubling behaviors regarding Internet regulation around the world.[19] Accordingly, ISPs are growing wary of complying with the Privacy Act's blocking provision and the MLAT process in general.[20] For example, some countries are seeking work-arounds, such as requiring "backdoor" access to encrypted programs and devices and asserting their legal right to unilateral access to the data, whereby relying on the MLAT process is unnecessary.[21] Finally, many countries have enacted, introduced, or considered laws that would limit the storage, movement, and/or processing of data to specific geographies or jurisdictions.[22] These different responses are problematic in many ways which are detailed below.

### A. *Threatening ISPs*

Foreign governments seeking access to American-held data essentially have two avenues at their disposal: the ISPs themselves or the MLAT process. ISPs and technology companies want to get along with foreign governments for a number of reasons, and it can be assumed that they comply with these sharing requests whenever possible.[23] Given that the MLAT process is so inefficient, foreign governments are increasingly pressuring ISPs to share information in ways that are dubious in their legality.[24] Google executives have even been arrested or detained in numerous countries under the auspices of violating local

---

[19] *See, e.g.*, Kyle Wagner, *A Brief History of Google Employees Being Arrested in Foreign Countries*, GIZMODO (Sept. 27, 2012), http://gizmodo.com/5947043/a-brief-history-of-google-employees-being-arrested-in-foreign-countries [https://perma.cc/L3DY-LVYR] ("Google executives get held in foreign countries that have a beef with Google.").

[20] *See* Ellen Nakashima & Andrea Peterson, *The British Want To Come to America – with Wiretap Orders and Search Warrants*, WASH. POST (Feb. 4, 2016), https://www.washingtonpost.com/world/national-security/the-british-want-to-come-to-america--with-wiretap-orders-and-search-warrants/2016/02/04/b351ce9e-ca86-11e5-a7b2-5a2f824b02c9_story.html?utm_term=.02d598a63d01 [https://perma.cc/HVF2-G2BX]; *see also* CYBERCRIME CONVENTION COMM. (T-CY), *supra* note 17, at 12 ("There is a trend among providers not to cooperate with criminal justice officials even when permitted by law to do so.").

[21] Daskal, *supra* note 8, at 476–78.

[22] Jonah Force Hill, The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders 3–4 (May 1, 2014) (unpublished paper presented at Hague Institute for Global Justice Conference on the Future of Cyber Governance), https://ssrn.com/abstract=2430275 [https://perma.cc/2C36-X8XK].

[23] *See, e.g.*, Andrew K. Woods, *Why Does Microsoft Want a Global Convention on Government Access to Data?*, JUST SECURITY (Feb. 19, 2014), https://www.justsecurity.org/7246/microsoft-global-convention-government-access-data/ [https://perma.cc/4VK5-5L84] ("Microsoft operates largely at the pleasure of local governments around the world, and reforming MLAT promises to improve these relationships.").

[24] *See id.* (describing how companies like Microsoft face enormous pressure from foreign governments to forego the MLAT process and hand over information directly).

privacy laws, a practice which is considered by some to be a "power play" against the company for its strict compliance with the Privacy Act and MLAT process.[25] Companies also claim that they are feeling pressure to capitulate to the requests from foreign governments or face the prospect of losing large government contracts.[26] While it appears that many American firms have refused to turn over data in ways that violate domestic law, industry insiders insist that they may soon no longer be able to do so.[27]

### B. *Backdoor Encryption Regimes and Claims for Unilateral Access to Data*

Many governments have begun to insist that new encryption technologies be designed with an avenue for "backdoor" government access so that law enforcement agencies can access data that would otherwise only be available through the MLAT process.[28] This would allow law enforcement access to a large amount of data, such as time and duration of photo calls, photos, and emails to the cloud.[29]

Additionally, some countries, like Brazil and the United Kingdom, have begun to pass laws which assert their authority to access or seize data from ISPs unilaterally, so long as those ISPs do any business or have any customers in the country.[30] Such legislation potentially forces ISPs to face a conflict of laws between two or more countries about whether and how to provide the requested data.[31]

### C. *Data Localization*

Perhaps the most controversial response has been data localization laws. Data localization laws "limit the storage, movement, and/or processing of data to specific geographies and jurisdictions, or . . . limit the companies that can manage data based upon the company's nation of incorporation or principal" place of business.[32] More than twelve countries, including Germany, Brazil, India, Indonesia, Australia, Canada, France, Malaysia, Russia, and China, have considered or adopted data localization laws.[33] Proposed data localization laws

---

[25] *See* Wagner, *supra* note 19.

[26] Hill, *supra* note 22, at 4.

[27] Nakashima & Peterson, *supra* note 20.

[28] *See* Peter Swire & Justin Hemmings, *Stakeholders in Reform of the Global System for Mutual Legal Assistance*, *in* SYSTEMATIC GOVERNMENT ACCESS TO PRIVATE SECTOR DATA 395, 399 (Fred H. Cate & James A. Dempsey eds., 2017).

[29] *Id.* at 401.

[30] Daskal, *supra* note 8, at 477.

[31] *Id.* at 477–78.

[32] Hill, *supra* note 22, at 3.

[33] *See generally id.* (providing a sampling of specific countries' proposed or enacted data localization laws).

vary greatly, and can consist of anything from limitations on data storage and transfer, to mandatory local ownership of data storage equipment, to broader localization rules which apply to *all* citizen data.[34] On the whole, such laws are impractical, problematic, and even counterproductive.

### 1. *Data Localization Laws Are Impractical*

Modern computing and data storage is possible because of its flexibility and efficiency in transferring data.[35] Critical storage infrastructure is not designed to operate in the ways that data localization laws mandate.[36] Oftentimes, localization laws necessitate that firms establish data storage centers within the legislating country, but there are still relatively few storage facilities worldwide.[37] Companies are very particular about the locations of their data storage servers, the operation and security of which are absolutely crucial for their business models.[38] For example, Google reportedly decided to locate a storage facility in Ireland because of the country's "highly educated, young, English-speaking workforce," relatively low corporate tax rate, and colder climate which lowers energy costs associated with keeping servers from overheating.[39] Additionally, there are strong arguments to be made that data localization laws make operations prohibitively expensive for foreign firms operating in different countries.[40] In developing countries where Internet access and data services are significant drivers of economic growth, disruptions in the free flow of data could preclude trillions of dollars in future GDP growth.[41]

---

[34] *Id.* at 3–4.

[35] *See* Dillon Reisman, *Where Is Your Data, Really?: The Technical Case Against Data Localization*, LAWFARE (May 22, 2017), https://www.lawfareblog.com/where-your-data-really-technical-case-against-data-localization [https://perma.cc/JC62-7C6H].

[36] *See* Hill, *supra* note 22, at 28–29 (describing the current use of the "best effort delivery model, where data is delivered to its destination in the most efficient manner possible, without predetermined routes").

[37] *See, e.g.*, *Data Center Locations*, GOOGLE, http://www.google.com/about/datacenters/inside/locations/index.html [https://perma.cc/6VDT-FZF3] (showing Google's limited data storage centers outside the United States). For an examination of a modern U.S. data center, see Rich Miller, *Microsoft's $1 Billion Data Center*, DATA CTR. KNOWLEDGE (Jan. 31, 2013), http://www.datacenterknowledge.com/archives/2013/01/31/microsofts-1-billion-roofless-data-center/ [https://perma.cc/M52X-S7BV].

[38] *See* Reisman, *supra* note 35 (describing how, in order to maintain a high degree of data integrity and reliability, companies require data to be backed up in multiple different data centers and regions).

[39] Henry McDonald, *Ireland Is Cool for Google as Its Data Servers Like the Weather*, GUARDIAN (Dec. 22, 2012), https://www.theguardian.com/technology/2012/dec/23/ireland-cool-google-data-servers-weather [https://perma.cc/5JN7-HYYZ].

[40] Hill, *supra* note 22, at 6, 26.

[41] *Id.* at 27.

### 2. *Data Localization Laws Are Problematic for Privacy and Civil Rights*

Civil society groups and human rights activists are often quick to point to the current Internet regulatory regime as problematic for privacy and civil rights.[42] These critiques are certainly not without merit in many respects, but data localization ironically poses a greater danger to civil rights and liberty than the status quo. Although there are legitimate reasons for foreign governments to pursue data localization policies, including economic and law enforcement benefits,[43] nations will be in a better position to collect information on their citizens, control the content of information that reaches their citizens, and censor the media or political opposition.[44] Indeed, collection alone can be used to stifle expressive, associational, and related rights.[45] When data is localized entirely within one country, the local governing authorities can, if they so desire, go so far as to shut down Internet services if they believe those services are aiding political opposition groups.[46] The existing worldwide Internet regime is by no means perfect, particularly in the ways in which it intersects with privacy and civil rights, but data localization policies are not the silver bullet for solving those problems.

### 3. *Data Localization Laws Are Counterproductive*

Data localization is often supported in part on the assumption that it will result in enhanced data security, but little evidence exists to support that assumption.[47] Data security is ultimately a function of security safeguards at the storage facility, rather than a function of the location of the data.[48] There are even indications that several countries considering data localization policies, like Brazil and Indonesia, "are actually among the least well-equipped nations to protect their data."[49] While it is true that data located in the United States is potentially subject to collection by the National Security Agency (NSA),[50] locating and retrieving data extraterritorially usually is subject to even weaker controls than those of the NSA.[51] Even if foreign intelligence agencies like the NSA were impeded by data localization, *domestic* intelligence agencies,

---

[42] *See Privacy*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/privacy [https://perma.cc/JUS8-XT5B] ("National and international laws have yet to catch up with the evolving need for privacy that comes with new digital technologies.").

[43] Hill, *supra* note 22, at 19.

[44] *Id.* at 28.

[45] Daskal, *supra* note 8, at 481.

[46] Hill, *supra* note 22, at 23.

[47] Reisman, *supra* note 35 ("The push for data localization requirements . . . reflects an inaccurate understanding of the Internet.").

[48] Hill, *supra* note 22, at 24–25.

[49] *Id.* at 26.

[50] *See* Daskal, *supra* note 8, at 498 n.79 ("[T]he NSA is likely to have much more information at its disposal on any given target than most foreign law enforcement.").

[51] Hill, *supra* note 22, at 25.

including those with little domestic oversight, or scant respect for civil rights, would be given access to much more potentially sensitive information than ever before.[52] Newer and smaller Internet providers would be left to determine whether and how to comply with law enforcement requests for data.[53] They would also be significantly less capable of fending off cyber intrusions from known cyber actors like Russia and China[54] Therefore, the arguments for data localization that hinge on the security benefits ignore the fact that data stored in-jurisdiction may actually be less secure and more accessible to privacy violations from intelligence agencies foreign and domestic.

## III. BILATERAL DATA SHARING AGREEMENTS

There are arguments that the best way to fix the MLAT process is to amend the Privacy Act in ways that would allow ISPs more flexibility to comply with law enforcement requests from foreign governments.[55] If ISPs were able to share more information with foreign governments, then the DOJ would receive fewer MLA requests, which would lead to greater efficiency.[56] Amending the Privacy Act's blocking provision in strategic ways could ostensibly increase the quantity and quality of data flow across borders, without compromising international human rights.[57] There are also related arguments in favor of separate bilateral treaties between relatively like-minded countries to allow a freer flow of data.[58] Such bilateral agreements might be more realistic because they require buy-in from fewer stakeholders, stakeholders that the United States can be confident are committed to the rule of law and privacy protections.[59]

---

[52] *See supra* notes 42–43.

[53] Hill, *supra* note 22, at 26.

[54] *See id.* at 26 n.105.

[55] *See generally* Andrew Keane Woods, *The Simplest Cross-Border Fix: Removing ECPA's Blocking Features*, LAWFARE (June 15, 2017), https://www.lawfareblog.com/simplest-cross-border-fix-removing-ecpas-blocking-features [https://perma.cc/QB8U-HZBX].

[56] Andrew Keane Woods, *Procedural Options for Improving Cross-Border Requests for Data*, LAWFARE (Oct. 13, 2015), https://www.lawfareblog.com/procedural-options-improving-cross-border-requests-data [https://perma.cc/2UR6-3WRF] ("The pressure on the MLAT system—thousands of MLA requests being routed through the DOJ—is the direct result of the Electronic Communications Privacy Act (ECPA). If ECPA did not require foreign law enforcement officers to get a US warrant in order to compel data, those officers would never need to request mutual legal assistance in the first place. The best way to resolve the MLA problem, then, is not to speed up the handling of MLA requests, but to end ECPA's requirement that all requests got [sic] through the MLA process.").

[57] *Id.*

[58] *Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era: Hearing Before the H. Comm. on the Judiciary*, 115th Cong. 4 (2017) (statement of Andrew Keane Woods, Assistant Professor, University of Kentucky College of Law).

[59] *See* Woods, *supra* note 56 ("Anyone with even passing familiarity with [I]nternet governance debates knows that the topic is highly politicized and achieving agreement between the major powers is extremely difficult. Even the relatively benign cybercrime treaty found non-universal adherence among like-minded western countries and no

Bilateral agreements would also require Congress to amend the Privacy Act, albeit in a more limited or targeted way. In fact, the DOJ has recently proposed legislation that would authorize such an agreement between the United States and the United Kingdom (U.S.–U.K. Agreement).[60] The proposed Agreement would be the first of its kind and an important introductory step to reforming the Privacy Act and, therefore, the MLAT process.[61]

As it stands now, major American Internet providers interpret the Privacy Act's blocking provision in one of two ways. Google and Facebook interpret it as prohibiting them from turning over any content data to any foreign government, regardless of the location of the data.[62] Microsoft, on the other hand, interprets the blocking provision as hinging on the location of the data.[63] Under this interpretation, Microsoft will disclose data if it is located in a country with jurisdiction to make the request.[64] Importantly, the Privacy Act does not prohibit ISPs from sharing non-content data, which is often referred to as "metadata," with foreign governments—even as U.S. law enforcement agencies remain required to seek court approval under the Fourth Amendment probable cause standard.[65]

## A. *U.S.–U.K. Agreement*

The United Kingdom is an ideal partner for the first data-sharing agreement for a number of reasons, including its commitment to democracy and rule of law.[66] Edward Snowden's disclosures about Project TEMPORA, which was a collaboration between the NSA and the Government Communications Headquarters (GCHQ), the British signals intelligence agency, revealed that the United Kingdom has been a close intelligence partner with the United States

---

accessions by major non-western countries. Add to this the questions of sovereignty, due process, and privacy rights and you have a recipe for deep divisions between many of the most important countries. For example, it is simply unlikely that the US and China will agree to the same set of due process provisions regarding cross-border law enforcement access to cloud data. Forging an international agreement that satisfies India, China, Brazil, Russia, and the US will likely be so watered down, it would have little utility; in fact, there is a serious risk that the resulting agreement would lead to an erosion of privacy rights, not an enhancement.").

[60] *See* Scarlet Kim & Greg Nojeim, *U.S. DOJ Cross-Border Legislation: Meeting Human Rights Requirements from Both Sides of the Pond*, LAWFARE (May 22, 2017), https://www.lawfareblog.com/us-doj-cross-border-legislation-meeting-human-rights-requirements-both-sides-pond [https://perma.cc/9VNC-RVYA].

[61] *See* Jennifer Daskal & Andrew K. Woods, *A New US-UK Data Sharing Treaty?*, JUST SECURITY (June 23, 2015), https://www.justsecurity.org/24145/u-s-u-k-data-sharing-treaty/ [https://perma.cc/6M5P-5KS9].

[62] Daskal, *supra* note 8, at 491.

[63] *Id.*

[64] *Id.*

[65] 18 U.S.C. § 2702(c) (2012).

[66] *See* Woods, *supra* note 56.

since the terrorist attacks on September 11, 2001.[67] United States officials have also concluded that the United Kingdom has "strong substantive and procedural protections for privacy," and that their legal standards have therefore not been at issue in discussions surrounding the proposed agreement.[68]

Any bilateral agreement would require that Congress amend provisions of the Privacy Act which otherwise block ISPs from sharing data with the U.K. In a letter to then-Senate President Joe Biden, then-Assistant Attorney General Peter Kadzik broadly outlined DOJ's legislative proposal for such an amendment.[69] Kadzik argues that "[r]eforming the MLAT process must remain a priority," but that agreements like the U.S.–U.K. Agreement would serve to streamline information sharing while alleviating some of the MLAT backlog, which he calls "unsustainable."[70] The letter also openly acknowledges that the proposed agreement would establish a framework that can be used in the future to enter into similar agreements with other countries, although there has been nothing to indicate that additional countries are being considered as potential partners at this point.[71]

The proposed legislation would amend sections of the Privacy Act, including the Wiretap Act, the Stored Communication Act (SCA), and the Pen/Trap Statute to allow ISPs to share both content data and non-content data (metadata) with foreign governments that have been "certified" by the U.S. Attorney General, with the concurrence of the Secretary of State.[72] In order to gain certifications, foreign governments must meet a long list of specific conditions, including (1) guaranteed baseline protections of privacy and civil liberties, (2) minimization of data collection of U.S. persons or domiciliaries, and (3) a laundry list of technical security controls and procedures.[73]

---

[67] *See* Hill, *supra* note 22, at 5; *see also* Nick Hopkins, *From Turing to Snowden: How US-UK Pact Forged Modern Surveillance*, GUARDIAN (Dec. 2, 2013), https://www.theguardian.com/world/2013/dec/02/turing-snowden-transatlantic-pact-modern-surveillance [https://perma.cc/R29K-YX7K] (discussing the relationship between the GCHQ and NSA, along with the beginning of intelligence programs after September 11, 2001).

[68] Nakashima & Peterson, *supra* note 20.

[69] Letter from Peter J. Kadzik, Assistant Attorney Gen., U.S. Dep't of Justice, to Joseph R. Biden, President, U.S. Senate 1–3 (July 15, 2016) [hereinafter Letter from Peter J. Kadzik], http://www.netcaucus.org/wp-content/uploads/2016-7-15-US-UK-Legislative-Proposal-to-Hill.pdf [https://perma.cc/2ARN-V9UP].

[70] *Id.* at 2.

[71] *Id.*

[72] *Section-by-Section Analysis of Legislation To Permit the Secure and Privacy-Protective Exchange of Electronic Data for the Purposes of Combating Serious Crime Including Terrorism*, *in* Letter from Peter J. Kadzik, *supra* note 69, at 1 [hereinafter *Analysis of DOJ Proposal*].

[73] *Id.* at 2–3.

### 1. *Privacy Protections*

In order to qualify for access to American-held data, the U.S. Attorney General must certify that the foreign government's (here, the United Kingdom's) domestic law "affords robust substantive and procedural protections for privacy and civil liberties."[74] The proposed legislation specifies the minimum baseline protections that must be in place, including domestic protections that are consistent with Chapters 1 and 2 of the international Budapest Convention on Cybercrime, as well as a "demonstrate[d] respect for the rule of law," "principles of non-discrimination," "international universal human rights," and the continued "global free flow of information."[75]

### 2. *Data Minimization*

DOJ's proposed legislation would also require that the U.S. Attorney General and Secretary of State certify that any foreign government has adopted "appropriate procedures" to ensure that information concerning U.S. persons is only acquired, retained, or disseminated in the most minimal way possible.[76] The foreign government may not target U.S. persons, nor may the foreign government target a non-U.S. person for purposes of obtaining information concerning a U.S. person.[77] Also, the foreign government may not request information in order to share it with third-party countries or even with the United States.[78]

### 3. *Controls and Procedures*

The proposed legislation elaborates on the requirements that countries must comply with in order to receive certification by providing sixteen specific provisions regarding the procedures with which data is to be collected, retained, and transferred.[79] These provisions include, in part, the following requirements:

- Requests must be related to "serious crime[s]" like terrorism;
- The request must pertain to a target (whether it be a specific person, a bank account, or an electronic device) that is specific and identifiable rather than engage in bulk-collection;

---

[74] *Legislation To Permit the Secure and Privacy-Protective Exchange of Electronic Data for the Purpose of Combating Serious Crime Including Terrorism*, *in* Letter from Peter J. Kadzik, *supra* note 69, at 3 [hereinafter *DOJ Legislative Proposal*]; *see also Analysis of DOJ Proposal*, *supra* note 72, at 2.

[75] *DOJ Legislative Proposal*, *supra* note 74, at 3–4.

[76] *Id.* at 4.

[77] *Id.*

[78] *Id.* at 5.

[79] *Id.* at 4–6; *see also Analysis of DOJ Proposal*, *supra* note 72, at 3–4.

- The request must be grounded on a "reasonable justification based on articulable and credible-facts";
- The request must be subject to independent review;
- The request "must be for a fixed and limited duration" that is "no longer than reasonably necessary to accomplish its approved purpose";
- The requests "may not be used to infringe freedom of speech";
- The foreign government must delete information that is "relevant to the prevention…or prosecution of serious crime[s]" or to protect against serious harm;
- "[T]he foreign government may not disseminate the content of a communication" of a person to United States authorities unless it "relates to significant harm" to the United States;
- The foreign government must reciprocate data access to the United States.[80]

The proposed legislation is still under consideration. There is no guarantee that the text as originally proposed would ultimately become the relevant law. That said, apart from a few specific areas of ambiguity, the legislation is commendable in its straightforward and thorough articulation of the requirements that the U.S. Attorney General must find to be satisfied before certifying a foreign government as a data-sharing partner.

### a. *Pros of the Proposed Legislation*

Any analysis of the proposed legislation must first acknowledge that the text of the actual agreement (as opposed to the text of the DOJ's legislative proposal) between the United States and United Kingdom has not been made public,[81] and that unless and until it is, all analyses regarding its merit cannot be comprehensive. Still, this proposed legislation gets many things right as far as reforms. First, requiring that the foreign government has acceded to the Budapest Convention on Cybercrime, or passed similar laws that put that government in accordance with the Convention,[82] ensures the potential data-sharing partner is like-minded in its commitment to a fair process of data collection and dissemination. The Budapest Convention, which has been accepted by over fifty countries including the United States, attempts to harmonize substantive laws internationally as they relate to cybercrime offenses, and provide standards for criminal procedural law that comport with international human rights and liberties.[83]

---

[80] *DOJ Legislative Proposal*, *supra* note 74, at 1, 7.

[81] Kim & Nojeim, *supra* note 60.

[82] *DOJ Legislative Proposal*, *supra* note 74, at 3–4.

[83] *Details of Treaty No. 185: Convention on Cybercrme*, COUNCIL EUR. TREATY OFF., https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 [https://perma.cc/CXG7-7DRF].

Next, the legislation's requirement that a request from a foreign government be subject to review or oversight by "a court, judge, magistrate, or other independent authority" is crucial to ensure that data requests comport with relevant privacy and national security laws in the requesting country.[84] Various European legal decisions have recently highlighted the necessity for independent review.[85] The proposed legislation's inclusion of an independent review requirement is therefore consistent with American laws and recent trends in European law.[86] Requiring independent review also serves to ensure that other requirements from the proposed legislation are met, including that requests be "based on articulable and credible facts," as well as that the request be of a limited and reasonable duration.[87]

Finally, the proposed legislation is right to forbid foreign governments from requesting information pertaining to U.S. persons or domiciliaries. Instead, foreign data-sharing partners would continue to rely on the MLAT process, and all of the bureaucratic checks and balances attendant with it, in order to access information on Americans. The legislation even contemplates that incidental collection of data from U.S. persons will almost certainly take place, but accounts for that collection by requiring that the foreign country minimize such data to the extent practicable and that they not share that data with either the United States or any other third-party country.[88]

### b. *Cons of the Proposed Legislation*

There are ambiguities and omissions within the text of the proposed legislation that have given privacy advocates cause for concern. For instance, although the proposed legislation requires that requests be subject to review or oversight by an "independent authority," it does not require that the request be issued by a court.[89] Currently the "Judicial Commissioners" in the United Kingdom, who review the U.K. Secretary of State's authorization for surveillance, approve warrants and requests so long as they find that it is "necessary" for national security and "proportionate" to the intrusion.[90] The United Kingdom's Judicial Commissioners are appointed to three-year terms by the prime minister, which raises questions about their independence.[91] Privacy skeptics point to the fact that the U.S. Department of Justice has consistently taken the position that government surveillance under the Foreign Intelligence Surveillance Act (FISA) is subject to "oversight" from FISA Courts, even though those courts merely approve

---

[84] *DOJ Legislative Proposal*, *supra* note 74, at 5.
[85] Kim & Nojeim, *supra* note 60.
[86] *Id.*
[87] *DOJ Legislative Proposal*, *supra* note 74, at 6.
[88] *Id.*
[89] Kim & Nojeim, *supra* note 60.
[90] *Id.*
[91] *Id.*

guidelines which govern *some* aspects of government surveillance,[92] as evidence that ostensible oversight mandated by the proposed legislation might not be all that strong, or all that independent. The proposed legislation's insistence that any requests be based on a "reasonable justification" has also been met with some skepticism.[93] Unless the Agreement is released to the public prior to the legislation's consideration, skeptics will probably not be satisfied.

Additionally, the proposed legislation is notable for its omission of any requirement that targets of surveillance be notified of that surveillance after the fact. U.S. law requires after-the-fact notice of any real-time surveillance, however U.K. law does not.[94] Still, recent decisions by the European Court of Human Rights and the European Court of Justice have spotlighted and underscored the necessity of notice as a means for people to seek a legal remedy if their rights or liberties have been infringed.[95] These decisions track with current U.S. law by requiring notification once it can be provided without jeopardizing the purpose of the surveillance or investigation.[96]

Lastly, the proposed legislation grants a significant amount of authority to the U.S. Attorney General, and thus the executive branch, without any clearly designated role for oversight from other branches of government.[97] Indeed, the legislation stipulates that any certifications made by the U.S. Attorney General "shall not be subject to judicial or administrative review."[98] Instead, the legislation requires only that the U.S. Attorney General give sixty days' notice to the House and Senate judiciary and foreign affairs committees prior to making a determination regarding certification.[99] By excluding the Agreement from judicial and administrative review, and failing to provide a mechanism for meaningful congressional oversight, the Agreement vests significant and novel authority in unelected officials of the executive branch.

## IV. SUGGESTIONS FOR REFORM

The current information-sharing regime is unsustainable. Modest improvements to the process and administration of MLATs are a necessary first step for supporting foreign law enforcement agencies and discouraging problematic behaviors like data localization. Simultaneously, however, there needs to be a more comprehensive long-term reform of the current MLAT framework. There are several viable options for potential reforms, each providing unique benefits and posing different challenges. While any of these

---

[92] *Id.*

[93] *Id.* (questioning the standard for its ability to be interpreted too broadly, thereby leading to an absence of a requirement for strong factual basis for surveillance).

[94] *Id.*

[95] *See* Kim & Nojeim, *supra* note 60.

[96] 18 U.S.C. § 2705(a) (2012) (delayed notice).

[97] *DOJ Legislative Proposal*, *supra* note 74, at 6.

[98] *Id.*

[99] *Id.*

options would be preferable to maintaining the status quo, this Essay advocates a more cautious and narrow set of changes to the framework in order to test them before instituting policies and procedures that dramatically transform the way that data is shared internationally.

## A. *Three Possible Short-Term MLAT Improvements*

There is a set of problems in the MLAT process that exacerbate the already difficult data-sharing process, such as a lack of a standardized online process, a lack of guidance to requesting countries, and a lack of adequate staffing and funding at the U.S. Department of Justice's Office of International Affairs (OIA).[100] These problems have relatively straightforward solutions, which were outlined in part by a 2013 President's Review Group on Intelligence and Communications Technologies but have not yet been implemented.[101] The improvements fall into the following three categories: (1) streamlining the application process; (2) raising awareness domestically and abroad; and (3) devoting more money and manpower to OIA.

### 1. *Streamlining*

First, there are simple, practical, and straightforward ways to streamline the MLAT application process. Incredibly, MLA requests are still submitted in hardcopy form, and there is no standard template provided in order to demonstrate what an adequate request looks like, nor anything in the way of guidance or instructions on the OIA website.[102] This is far from ideal, as there is no reason to expect foreign law enforcement stakeholders, like a local police department in Ireland, to be familiar with the MLAT process, or to be well-versed enough in American Fourth Amendment jurisprudence to provide details adequate to show probable cause. Indeed, the OIA often has to send back MLA requests to foreign governments because of the requests' inability, without more, to satisfy a magistrate judge's determination of probable cause.[103] Providing instructions and a template for data requests would be a simple way to ensure the quality and consistency of requests and alleviate a major source of inefficiency in the MLAT process.

Another way to streamline the MLAT process would be to take measures to designate specific attorneys at USAO, and/or specific district courts to handle MLAT requests.[104] Peter Swire and Justin Hemmings report that interviews with officials involved in the process blame lengthy request response times on the fact that requests are regularly assigned to Assistant U.S. Attorneys that lack familiarity with MLA requests and are typically also handling a full docket of

---

[100] Swire & Hemmings, *supra* note 9, at 718, 722–23.
[101] *Id.* at 700 n.54.
[102] *Id.* at 722.
[103] Daskal, *supra* note 8, at 483.
[104] Swire & Hemmings, *supra* note 9, at 718–20.

other, more local, assignments.[105] Federal magistrate judges appear similarly ignorant.[106] Part of the reason for this problem is that the current process refers requests to the federal district where the data is actually being held,[107] even though a 2009 amendment to the Privacy Act allows *any* federal court to issue a warrant, anywhere in the nation.[108] The current system of farming out MLA requests to attorneys who are unfamiliar with the process, in any number of federal districts that have no particular reason to be aware of MLATs at all, is a paragon of inefficiency.

### 2. *Raising Awareness*

Raising awareness about the MLAT process would not only improve the quality and consistency of requests, but also increase the speed with which those requests are processed.[109] It would also promote transparency at home and abroad; assuage lingering frustrations in the international law enforcement community; and perhaps disincentivize problematic unilateral action, like data localization policies, on the part of foreign governments.[110] Any efforts to raise awareness must include providing resources such as templates, guidance, and training about how to make, track, and execute data requests.

### 3. *Increasing OIA Funding*

Finally, and perhaps most straightforwardly, the OIA needs increased funding and staff. DOJ itself has publicized that while MLA requests for assistance have increased dramatically, government resources "have not kept pace."[111] The 2013 Presidential Review Group report recommended providing OIA more resources, and proposed budgets for 2015,[112] 2016,[113] and 2017[114]

---

[105] *Id.* at 718.

[106] *Id.* at 719.

[107] *Id.* at 718.

[108] *Id.* at 719.

[109] *Id.*

[110] *See* Swire & Hemmings, *supra* note 9, at 723–24 (noting that publicizing and supporting an improved MLA process would be innovative and efficient and would discourage governments from seeking other ways to compensate for their inability to conduct wiretaps on Internet communications).

[111] U.S. DEP'T OF JUSTICE, FY 2015 BUDGET REQUEST: MUTUAL LEGAL ASSISTANCE TREATY PROCESS REFORM + 24.1 MILLION IN TOTAL FUNDING (2015), https://www.justice.gov/sites/default/files/jmd/legacy/2014/07/13/mut-legal-assist.pdf [https://perma.cc/8GZE-MQDR].

[112] *Id.*

[113] U.S. DEP'T OF JUSTICE, GENERAL LEGAL ACTIVITIES CRIMINAL DIVISION: FY 2016 BUDGET REQUEST AT A GLANCE [hereinafter U.S. DEP'T OF JUSTICE, FY 2016], https://www.justice.gov/sites/default/files/jmd/pages/attachments/2015/01/30/12_bs_section_ii_chapter_-_crm.pdf [https://perma.cc/24DJ-C9TP].

[114] U.S. DEP'T OF JUSTICE, FY 2017 BUDGET REQUEST AT A GLANCE, https://www.justice.gov/jmd/file/821916/download [https://perma.cc/LZZ6-RUGP].

have all recommended increases in the number of attorneys and the amount of money that OIA should receive, though those numbers have varied considerably.[115] While the Fiscal Year 2019 proposed budget may be the most modest request to date, OIA still requested adding seventy-two staff members and a funding increase of over $10 million.[116] Previous requests have failed to receive congressional approval generally, though smaller, more specific parts of requests have been approved.[117] Without increased resources, OIA will continue to flounder under its heavy backlog and constant influx of foreign MLA requests.[118] With OIA's heavy backlog, the international law enforcement community will continue to seek alternative and potentially deleterious data-collection policies.[119]

## B. *Four Possible Long-Term MLAT Reforms*

As noted above, short-term reforms to the MLAT process should be coupled with more dynamic reform in the ways that ISPs can comply with the growing international demand for information. There are at least four promising avenues for reform which all require a similar set of actions from Congress. While this Essay briefly elaborates on all four potential reform mechanisms, it asserts that it is in the best long-term interest of the United States, global Internet users, and Internet Service Providers that any significant reforms be done in a conscientious and intentional way. Accordingly, this paper ultimately recommends a slow start to reform, one that focuses explicitly and exclusively on sharing data with the United Kingdom as a pilot program before enacting sweeping reforms. By allowing data sharing with only the United Kingdom, and not opening the door to any other foreign partnerships, the United States can test the policy outcomes of the new reforms without completely abandoning the status quo or fundamentally altering the current international Internet privacy regime before we know where that will lead.

### 1. *Amend the Privacy Act Broadly*

The most dramatic way to reform the MLAT process would be to rewrite the Privacy Act without provisions that block ISPs from sharing data with

---

[115] For example, the Office of International Affairs formally requested, for Fiscal Year 2016, 141 additional staff members, including seventy-seven attorneys, and over $32 million increase in funding. U.S. DEP'T OF JUSTICE, FY 2016, *supra* note 113.

[116] U.S. DEP'T OF JUSTICE, GENERAL LEGAL ACTIVITIES CRIMINAL DIVISION (CRM): FY 2019 BUDGET REQUEST AT A GLANCE, https://www.justice.gov/jmd/page/file/1033246/download [https://perma.cc/YP6L-LQL8] ("This support is imperative to avoid further backlogs in the critical support provided by OIA to protect the United States and support U.S. Attorneys' Offices, as well as our state and local law enforcement partners.").

[117] Swire & Hemmings, *supra* note 9, at 717.

[118] *Id.* 716.

[119] *Id.*

foreign governments. Congress could add sections to the Wiretap Act, the Stored Communications Act, and the Pen/Trap Statute that detail when and under what circumstances providers may comply with foreign requests for assistance. There are myriad ways to write such amendments, and many ways that they could safeguard the privacy of American citizens. For instance, Congress could amend sections of the statute to only allow for the exchange of information regarding users who are citizens of the requesting country, and only insofar as that information pertains to crimes committed within the country.[120]

However, such blanket amendments are ill-advised because of complications that will inevitably arise due to the conflicting criminal procedures in different countries, the growing globalization of crime, and the increased interconnectivity of Internet users.[121] What should be done, for example, when American citizens are implicated or incidentally monitored during the normal course of an investigation but *after* data has already been shared? What is to be done when requests for assistance involve citizens of multiple different, perhaps adversarial, jurisdictions? These examples should underscore the innumerable ways that developing trends in technology and the Internet are unpredictable and complex, which necessitates careful and narrow reforms to existing laws and policies.

### 2. *Bilateral Treaties and U.S.–U.K. Agreement Framework*

Bilateral treaties like the proposed U.S.–U.K. Agreement are more promising and less problematic than broad reforms to the Privacy Act because they are more specific. By articulating particular foreign countries that are suitable for data sharing outside of the MLAT framework, Congress could ensure that ISPs are only able to share data with trusted partners who have a demonstrated track record of sound criminal procedures and privacy laws. This more limited reform has the benefit of alleviating some of the pressures on the OIA and ISPs while maintaining the more managed MLAT process for other countries that make requests that implicate American citizens and domiciliaries. While the U.S.–U.K. Agreement is a good attempt to set baseline standards for future bilateral agreements, it must be improved in several important ways.

First, although the Agreement does necessitate that requests be reviewed for approval by an independent body, there must be a more specific definition of what the term "independent" requires.[122] In the United Kingdom, requests for surveillance are approved by Judicial Commissioners, who are appointed to their positions in three-year terms, making them less isolated from outside

---

[120] Daskal, *supra* note 8, at 499 n.80.

[121] *See* Andrew Keane Woods, *A Proposal To Improve Foreign Law Enforcement Access to US-Held Data*, JUST SECURITY (Sept. 30, 2015), https://www.justsecurity.org/26461/proposal-improve-foreign-law-enforcement-access-us-held-data/ [https://perma.cc/VH6C-W484].

[122] *See* Kim & Nojeim, *supra* note 60 (describing present ambiguities and distinctions between the United States and United Kingdom approaches).

pressures than would be preferred.[123] Data requests from law enforcement agencies are an infiltration into the private lives of Internet users and must only be made when necessary for valid law enforcement purposes. The costs inherent with potential privacy violations are too great to be entrusted to anyone who is not completely independent from public and political pressures. The U.S.–U.K. Agreement should acknowledge that cost by stipulating that MLA requests be reviewed by a member of the judicial branch.

Second, the Agreement must specify in greater detail what constitutes a "reasonable justification"[124] for data requests. Although the Agreement insists that such a justification be based on "credible facts, particularity, legality and severity,"[125] privacy proponents are right to criticize such requirements as too vague. In order to authorize surveillance or data collection from American companies, foreign governments must be held to a higher standard in justifying the necessity of their requests. This is not to say that other governments should be held to the unique American probable cause standard, only that more than a reasonableness test should be required.[126] Doing so would ensure that the privacy of global Internet users is only infringed when absolutely necessary.

Finally, the Agreement should require that targets be notified after the fact of their surveillance or data collection. It is irrelevant that U.K. law does not require notification, because it is America's prerogative to place reasonable regulations on the use of American-held data.[127] Requiring that targets be notified increases transparency, promotes accountability, provides for legal redress in the case of abuses, and, most importantly, comports with growing trends in European legal decisions that promote notification as a best practice.[128]

### 3. *Mutual Legal Assistance Statute*

An interesting alternative to bilateral treaties is the enactment of specific statutes which would govern legal assistance to foreign countries, rather than the existing regime of treaties. A Mutual Legal Assistance Statute (MLAS) is ostensibly preferable to a Mutual Legal Assistance Treaty (MLAT) because it is more flexible and more easily changed to account for the exigencies of the contemporary geopolitical situation.[129] Treaties are difficult to change, and

---

[123] *Id.*

[124] *DOJ Legislative Proposal*, *supra* note 74, at 5.

[125] *Id.* at 4.

[126] Woods, *supra* note 56.

[127] *See, e.g.*, Kim & Nojeim, *supra* note 60 ("At a minimum, it should be amended to require . . . notice to the targets of surveillance. Including such requirements is not 'American imperialism' as some critics have alleged, but rather are among the elements necessary to respect and promote international human rights standards.").

[128] *See supra* note 86.

[129] Swire & Hemmings, *supra* note 9, at 732–33.

mustering the political will to make such changes is rare.[130] Instead, MLAS would be relatively easy for the U.S. Congress to amend as it sees fit. Proponents of the MLAS approach point to the U.S. Visa Waiver Program (VWP) as an example.[131] The VWP was developed to address the ever-growing numbers of visa applicants to the United States and the difficulty with which U.S. Customs and Border Protection had with dealing with so many requests.[132] The VWP started slow, with only the countries most motivated to ease travel into the United States going to the trouble of complying with the requirements for the program, but has grown to accept numerous countries, though only those with the highest quality visa applications.[133] When the San Bernardino shooting demonstrated shortcomings in the VWP process, Congress amended the governing statute within days to add new requirements and controls.[134] MLAS proponents point to the speed and ease of substantively amending any potential MLAS as evidence of the virtue of such a plan.[135] An MLAS regime would be useful in many ways, but continues to pose sticky questions regarding when a country ought to be deemed adequate for inclusion to the program and when requests ought to be deemed adequate for bypassing the existing MLAT process. As mentioned above, more data is required before these questions can be answered in a satisfactory way. Instead, before dramatic changes to the existing data-sharing regime are made, the United States should enact less ambitious and more targeted reforms.

### 4. *Hybrid Bilateral Agreement/MLAS Approach*

Analysis of any of the potential reforms reveals that there are benefits to each, but also that beginning dramatic reforms prematurely could cause problems that render them counterproductive. Instead, the United States should proceed cautiously, with smaller scale reforms that measure outcomes before significant changes to the existing privacy regime take place. This Essay advocates for a hybrid bilateral agreement/MLAS approach, whereby the United States proceeds with the U.S–U.K. Agreement, but with an important corollary: explicitly limit the agreement to the United Kingdom, without providing any mechanism for further agreements for the time being. An exclusive agreement provides all of the efficiency benefits of other proposed reforms without any of the drawbacks. The OIA will see a significant reduction of the over 20,000 yearly requests for assistance from the United Kingdom,[136] and the global

---

[130] *See, e.g.*, Woods, *supra* note 56 ("Anyone with even passing familiarity with [I]nternet governance debates knows that the topic is highly politicized and achieving agreement between the major powers is extremely difficult.").

[131] Swire & Hemmings, *supra* note 9, at 726.

[132] *Id.* at 726–27.

[133] *Id.* at 729.

[134] *Id.* at 730.

[135] *Id.* at 730–31.

[136] *See* Woods, *supra* note 2, at 743–44.

privacy community can monitor the resulting outcomes before committing itself to more dramatic changes.

Rather than authorize the U.S. Attorney General and Secretary of State to certify countries as data-sharing partners, the authorizing legislation for the U.S.–U.K. Agreement should make narrow allowances for ISPs to comply with direct requests exclusively from the United Kingdom. Such legislation avoids vesting so much authority in the executive branch without mechanisms for oversight or review, as the current proposal would do. Such a legislative scheme would therefore achieve the flexibility that a MLAS would provide, while avoiding the sticky questions that an MLAS regime currently presents. Like the Visa Waiver Program, such an exclusive U.S.–U.K. Agreement could be easily expanded to include other countries, but only those countries who are most motivated to enact policies and procedures that make them ideal candidates for data-sharing. The United States is in a position of relative bargaining power currently as a result of the dominance of American ISPs and the proliferation of data held in American jurisdictions. Other countries will meet America halfway by making changes to their privacy policies that make them more attractive data-sharing partners, which will help ease the difficulty currently posed by evaluating the often varied and divergent privacy laws and criminal procedures of foreign governments.

Finally, such an exclusive agreement would provide the United States with more leverage to improve privacy policies regarding the collection of metadata. As mentioned previously, the current Privacy Act regime allows foreign governments to collect metadata directly from ISPs without limitation, even as American law enforcement is prevented from such access. As data collection and communication technologies evolve, rules that differentiate between content data and metadata are increasingly distinguishing between data types that do not have any differences.[137] Metadata can often be more personal and useful than content data,[138] and should be regulated accordingly. Countries like the United Kingdom seeking special access to American-held data should be required to accede to stricter metadata collection policies, and stipulating as such within new exclusive agreements could be an equitable compromise.

## V. CONCLUSION

The existing MLAT process needs reform. Until meaningful changes are made, the international community will continue to witness problematic behaviors on the part of governments and law enforcement agencies dissatisfied with the status quo. As has been shown, multiple avenues for change exist, though each poses its own benefits and drawbacks. The best way forward for

---

[137] *See* Swire & Hemmings, *supra* note 9, at 734 ("The importance of stricter legal standards for non-content in the United States has been prominently supported by consumer groups, technology companies, members of Congress, and other members of the Digital Due Process Coalition.").

[138] *See* Daskal, *supra* note 8, at 479.

the United States, however, is to proceed with modest reform by entering into an exclusive agreement with the United Kingdom with highly specific standards and requirements for the protection of human rights.

Entering into an agreement with the United Kingdom provides the United States with an opportunity to experiment with MLAT reform, without fundamentally altering the data-sharing status quo. By starting slow, the United States and the United Kingdom can identify potential problems and difficulties that may arise as both nations embark on a new and unpredictable privacy regime. This limited agreement would require compromises regarding criminal procedure, independent review of data-sharing requests, notification to targets of surveillance, and the use of metadata. All of these changes serve to strengthen privacy protections for Internet users worldwide, while promoting international law enforcement and alleviating some of the existing burden on the U.S. Department of Justice posed by the MLAT process.